International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ATTRIBUTE-BASED APPROACHES TO ENHANCE DATA SHARING SECURITY AND PRIVACY IN CLOUD ENVIRONMENTS

[1] *Zheng Ying Chen*,[2] *Sai Krishna*
Department of CSD
Harbin Institute of Technology, Harbin, China

Received: 01-01-2025 Accepted: 03-2-2025 Published: 13-2-2025

ABSTRACT

Cloud computing has become the backbone of modern digital ecosystems, enabling scalable storage, computation, and seamless data sharing across distributed environments. However, the proliferation of sensitive information in cloud platforms raises pressing concerns over privacy and unauthorized access. Traditional access control mechanisms often fail to address dynamic, fine-grained requirements of data owners in multi-user and multi-tenant contexts. In recent years, Attribute-Based Encryption (ABE) and related attribute-driven techniques have emerged as powerful paradigms to ensure confidentiality, flexible access control, and accountability in cloud-based data sharing. This paper investigates attribute-based approaches as a solution to strengthen data sharing security, offering resistance against unauthorized access, collusion attacks, and insider threats. By integrating attribute-based models with cryptographic primitives and policy-driven enforcement, the study aims to design a scalable and privacy-preserving framework that balances usability with robust protection. Experimental evaluations demonstrate the effectiveness of these approaches in minimizing overhead while maintaining strong security guarantees.

I. INTRODUCTION

The rapid adoption of cloud computing has redefined the way organizations and individuals manage data, shifting from local storage to distributed and outsourced infrastructures. While cloud platforms provide significant advantages such as elasticity, cost-efficiency, and accessibility, they also expose sensitive data to unprecedented risks of leakage, tampering, and unauthorized disclosure. Conventional encryption methods, while effective for static environments, often lack the granularity required in collaborative and heterogeneous cloud contexts. Attribute-Based Encryption (ABE) has emerged as a promising paradigm that embeds access control policies directly into cryptographic mechanisms, allowing data owners to define who can access data based on attributes such as roles, time, or location. Unlike identity-based approaches, ABE supports fine-grained, policy-centric, and scalable access management, making it particularly suitable for cloud environments. This research focuses on analyzing attribute-based models, highlighting their capacity to safeguard privacy while addressing emerging challenges such as computational efficiency, dynamic policy updates, and resistance against insider threats.

II. LITERATURE SURVEY

The literature on cloud security underscores the importance of fine-grained access control and privacy-preserving data sharing. Early works concentrated on Role-Based Access Control (RBAC), which, though efficient, suffered from rigidity in dynamic environments [1], [2]. To address this, Attribute-Based Encryption (ABE) was introduced by Sahai and Waters [3], establishing a cryptographic framework where access rights are tied to user attributes rather than fixed identities. Subsequent studies have proposed Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE), offering flexibility in delegating access based on data owner preferences [4], [5]. Extensions of ABE integrate mechanisms for revocation, accountability, and scalability to mitigate threats such as

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

collusion and key leakage [6], [7]. Recent works further explore hybrid frameworks combining ABE with blockchain and distributed ledger technologies to strengthen transparency and auditability [8], [9]. Additionally, research on privacy-preserving computation, such as homomorphic encryption and secure multi-party computation, has been incorporated into ABE-based schemes to enhance secure collaboration [10], [11]. Despite advancements, challenges remain in reducing encryption/decryption costs, supporting dynamic attributes, and ensuring interoperability in multi-cloud ecosystems [12]–[15]. These studies collectively suggest that attribute-based approaches represent a significant step toward robust, privacy-centric cloud security, though optimization for real-world deployment remains a critical area of inquiry.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

In traditional cloud environments, data sharing security and privacy have primarily been addressed using encryption-based schemes such as Role-Based Access Control (RBAC), Identity-Based Encryption (IBE), and conventional symmetric/asymmetric key distribution methods. While these systems provide a basic level of confidentiality and controlled access, they often rely heavily on centralized authorities to manage keys and policies. Moreover, data owners and users must trust the cloud service provider completely, which introduces vulnerabilities in terms of insider attacks and policy enforcement. Existing systems also lack fine-grained access control mechanisms that allow flexible and dynamic policy updates based on user attributes. As cloud services expand and multi-user collaborations become common, the shortcomings of these traditional methods make them inadequate for modern security and privacy requirements.

DISADVANTAGES

Limited Fine-Grained Control: Most existing encryption and access control models fail to support fine-grained, attribute-based conditions, leading to either over-privileged access or denial of legitimate requests.

Single Point of Failure: Centralized key management systems introduce bottlenecks and vulnerabilities, as compromise of the authority or key server can expose all sensitive data.

Poor Scalability and Flexibility: Traditional models struggle to handle dynamic environments where users, roles, and access policies change frequently, making them less suitable for large-scale cloud systems.

PROPOSED SYSTEM

The proposed system introduces an Attribute-Based Encryption (ABE) framework to enhance data sharing security and privacy in cloud environments. Unlike traditional role-based or identity-based mechanisms, the proposed system leverages user attributes such as roles, organizational units, or access contexts to dynamically determine access rights. This ensures that only authorized users who satisfy the defined attribute policies can decrypt and access sensitive data. The system incorporates Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for fine-grained access control, where data owners embed access structures directly into the ciphertext. In addition, the system adopts distributed key management to overcome the limitations of centralized authorities, ensuring resilience against insider threats and single points of failure. By integrating advanced cryptographic primitives and flexible policy definitions, the proposed system provides a scalable, privacy-preserving, and secure data sharing model for cloud environments.

ADVANTAGES

Fine-Grained Access Control: The use of attribute-based encryption allows data owners to enforce highly specific policies,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ensuring that access is granted only when all required attributes are satisfied.

Improved Security and Privacy: By decentralizing key management and embedding policies within the ciphertext, the system reduces reliance on cloud providers, mitigating risks of insider attacks and unauthorized data exposure.

Scalability and Flexibility: The system adapts easily to dynamic cloud environments, supporting policy updates, user revocations, and large-scale multi-user scenarios without significant performance degradation.

IV. PROPOSED METHODOLOGY

The proposed framework employs an Attribute-Based Encryption (ABE) scheme integrated with a cloud-based data sharing system to enforce fine-grained, policy-driven access control. The system architecture consists of three key entities: the data owner, the cloud service provider, and authorized users. Data owners encrypt sensitive data using CP-ABE, embedding access policies based on a predefined attribute set (e.g., role, department, clearance level). User secret keys are generated through a trusted attribute authority, ensuring that only those whose attributes satisfy the embedded policy can decrypt the content. To enhance security, a dynamic attribute revocation mechanism is incorporated, allowing real-time updates when user roles change or privileges are revoked. The methodology also integrates lightweight cryptographic techniques to reduce computational costs and applies privacy-preserving auditing for accountability. Furthermore, hybridization with blockchain-based logging mechanisms is proposed to maintain transparency in access events without exposing user identities. This holistic approach ensures confidentiality, privacy, and accountability while optimizing for scalability in multi-tenant cloud environments.

V. EXPERIMENTAL SETUP

The proposed system was implemented using a simulated cloud environment on Amazon Web Services (AWS) and OpenStack infrastructure. The encryption and decryption modules were developed using Python libraries supporting ABE and bilinear pairing-based cryptography. A dataset consisting of healthcare records and academic datasets with varying sensitivity levels was utilized to model real-world data sharing scenarios. User groups were assigned multiple attributes such as profession, location, and access level to test the flexibility of access policies. Experimental evaluation measured key performance metrics including encryption/decryption time, communication overhead, storage cost, and resistance to unauthorized access attempts. Comparative analysis was conducted against traditional RBAC and identity-based encryption models to evaluate efficiency and robustness. The system's auditing module was tested with a Hyperledger blockchain for logging access activities.

VI. RESULTS AND DISCUSSION

The experimental evaluation revealed that the proposed attribute-based framework significantly outperformed traditional RBAC and identity-based encryption models in terms of flexibility and security. The encryption and decryption overhead was found to be marginally higher than RBAC, but within acceptable ranges for real-world applications. Attribute-based revocation mechanisms demonstrated effectiveness in preventing unauthorized access in dynamic environments, reducing insider threat risks. The blockchain-audited logging framework further enhanced accountability by creating immutable access trails, ensuring transparency without disclosing user identities. A comparative study highlighted that while ABE introduces additional computational costs, the gains in privacy preservation and fine-grained access control

outweigh the trade-offs. The results also confirmed scalability in multi-user and multi-cloud scenarios, though performance optimizations in key generation and revocation remain areas for improvement. Overall, the attribute-based approach provides a robust solution for secure, privacy-preserving, and transparent data sharing in cloud environments.

VII. CONCLUSION

This study explored attribute-based approaches to enhancing data sharing security and privacy in cloud environments. By embedding access control policies directly into encryption, Attribute-Based Encryption (ABE) provides a robust, fine-grained, and scalable solution to the limitations of traditional security mechanisms. The proposed framework, integrating CP-ABE, dynamic attribute revocation, and blockchain-based auditing, ensures confidentiality, privacy, and accountability while maintaining scalability. Experimental evaluations validated the approach, demonstrating strong resistance against unauthorized access and insider threats with acceptable computational overhead. Future work will focus on optimizing cryptographic operations, enhancing attribute revocation mechanisms, and exploring cross-cloud interoperability. As cloud ecosystems evolve, attribute-based methods present a promising direction for achieving privacy-preserving, secure, and transparent data sharing.

REFERENCES

[1] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, “Role-based access control models,” Computer, vol. 29, no. 2, pp. 38–47, 1996.

[2] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli, “Proposed NIST standard for role-based access control,” ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, pp. 224–274, 2001.

[3] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. EUROCRYPT, 2005, pp. 457–473.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE S&P, 2007, pp. 321–334.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM CCS, 2006, pp. 89–98.

[6] M. Chase and S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. ACM CCS, 2009, pp. 121–130.

[7] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. ACM CCS, 2007, pp. 195–203.

[8] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably secure and efficient bounded ciphertext policy attribute-based encryption,” Inf. Sci., vol. 180, no. 3, pp. 257–270, 2010.

[9] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in Proc. IEEE SecureComm, 2010, pp. 89–106.

[10] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 743–754, 2012.

[11] S. Ruj, A. Nayak, and I. Stojmenovic, “Decentralized access control with anonymous authentication of data stored in clouds,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 384–394, 2014.

[12] K. Yang and X. Jia, “Attribute-based access control for multi-authority systems in cloud storage,” Proc. IEEE ICC, 2012, pp. 5360–5365.

[13] H. Zhu, X. Lin, R. Lu, and X. Shen, “ESPOON: Enforcing encrypted security

policies in outsourced environments," IEEE Trans. Serv. Comput., vol. 4, no. 4, pp. 282–295, 2011.

[14] Y. Zhang, R. Deng, J. Shu, and D. Zheng, "Attribute-based data sharing with flexible and direct revocation in cloud computing," IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 953–967, 2018.

[15] Q. Xia, E. Sifah, K. Asamoah, J. Gao, X. Du, and M. Guizani, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," Inf. Syst., vol. 81, pp. 1–13, 2019.